

CHARTRE INFORMATIQUE

FONDATION ILDYS

Préambule

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein de la Fondation ILDYS, en particulier de préciser les responsabilités des utilisateurs, ce conformément à la législation et afin de permettre un usage normal et optimal des ressources informatiques et des services Internet employés dans l'établissement.

Cette charte sera soumise à l'examen des instances représentatives du personnel le 16/02/2006 pour entrer en vigueur le 01/03/2006. Elle sera annexée au règlement intérieur de l'établissement. Une copie sera également transmise à l'inspection du travail et au secrétariat du Conseil des Prud'hommes de Morlaix. Ce texte est avant tout un code de bonne conduite.

DEFINITIONS

○ On désignera sous le terme « établissement » l'ensemble des lieux administrés par la Fondation ILDYS.

○ On désignera de façon générale sous le terme « ressources informatiques », les moyens informatiques de calcul ou de gestion locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'établissement. Il s'agit d'un ensemble comprenant le matériel, les logiciels standards et spécifiques, les moyens de communication.

○ On désignera par « services Internet », la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum...

○ On désignera sous le terme « utilisateur », toute personne, quel que soit son statut (salarié, vacataire, personnes mises à disposition, intérimaire, stagiaire, consultant,...), ayant accès ou utilisant les ressources informatiques, services Internet, téléphone fixe ou mobile.

○ On désignera sous le terme « administrateur réseau », les personnes du service informatique de l'établissement, qui veillent à assurer le fonctionnement normal et la sécurité des réseaux et systèmes.

La Fondation ILDYS met à la disposition de tout utilisateur des équipements informatiques, des moyens de communication, ainsi que des informations et données qui sont nécessaires à l'accomplissement de sa mission.

La Direction définit les conditions d'utilisation des systèmes informatiques de l'établissement (et notamment les conditions d'utilisation des logiciels, d'Internet et intranet...) afin de faire bénéficier les salariés des avancées technologiques réalisées en la matière tout en assurant la protection de l'intégrité de l'entreprise.

Cet objectif tend à être réalisé par une limitation de l'utilisation de l'outil informatique pendant le temps de travail et la mise en place d'un contrôle exercé par l'employeur sur les salariés utilisateurs, chaque salarié ayant été préalablement et personnellement informé de l'existence d'un tel contrôle.

Article 1 UTILISATION DES RESSOURCES INFORMATIQUES, DES SERVICES INTERNET ET DU RESEAU

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

L'activité professionnelle est celle prévue par les statuts du personnel auquel est lié l'établissement, à savoir : les activités de santé, mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.

Article 1.1 AUTORISATION D'UTILISATION

L'utilisation des ressources informatiques partagées de l'établissement et la connexion d'un équipement sur le réseau sont soumises à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers.

Ces autorisations peuvent être retirées à tout moment.

Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

Article 1.2 REGLES GENERALES D'UTILISATION, DE SECURITE ET DE BON USAGE

Les salariés sont tenus de conserver en bon état les biens, moyens et matériels mis à leur disposition par l'établissement. Ils se doivent de les utiliser de façon appropriée et conforme aux règles générales et particulières édictées par l'établissement.

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et à celle de l'établissement.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

L'utilisateur doit se conformer aux prescriptions suivantes (liste non exhaustive. Un manquement pourrait être considéré comme fautif ou abusif) :

- | | |
|--|--|
| <ul style="list-style-type: none">○ Il doit appliquer les recommandations de sécurité de l'établissement.○ Il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition.○ Il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.○ Il choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers.○ Il ne doit pas enlever les étiquettes des équipements. Il doit pas procéder à des inscriptions ou coller des documents sur les équipements sans demande préalable auprès du service informatique. | <ul style="list-style-type: none">○ Il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage.○ Il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité.○ Il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier les fichiers contenant des informations qui lui sont transmises.○ Il ne doit pas quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles. Il doit éteindre l'ensemble des équipements quand il termine son temps de travail (micro, écran et imprimante).○ Il doit alerter le service informatique s'il a accès à des données dont il n'est pas destinataire. |
|--|--|

Article 1.3 UTILISATION DE L'INTERNET, DE LA MESSAGERIE ET DE L'INTRANET

Compte tenu des risques inhérents à l'utilisation de l'Internet, de la messagerie et de l'intranet, les salariés doivent veiller en toutes circonstances à utiliser ces technologies dans les respects des règles élémentaires de sécurité, de bonnes moeurs et de bonne conduite et ce, par principe, dans le cadre exclusif de la réalisation de leurs missions professionnelles.

Ainsi, chaque utilisateur se doit de respecter notamment les règles d'utilisation définies ci-dessous, lesquelles ne font pas obstacle à l'exercice des prérogatives éventuellement reconnues dans le cadre du droit syndical.

Article 1.3.1 ACCES A INTERNET

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

L'utilisation de l'Internet est réservée à un usage professionnel. La durée de connexion ne doit pas excéder un délai raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener.

Dans tous les cas, l'utilisation de l'Internet ne doit pas revêtir un caractère fautif ou abusif. Sont notamment considérés comme fautifs ou abusifs les agissements suivants, sans que cette liste ne présente un caractère limitatif :

○ La consultation de site à caractère pornographique, xénophobe, raciste et, d'une façon générale, de tout site susceptible de mettre en jeu la responsabilité pénale de leurs concepteurs et/ou de leurs utilisateurs.

○ La répartition à des jeux d'argent ou de hasard, qu'ils soient licites ou illicites, ainsi que la réalisation d'opérations financières d'investissement ou à caractère spéculatif.

○ Le téléchargement de toutes informations et de tous logiciels ou documents, quelle que soit leur forme ou leur nature, à des fins personnelles.

○ Le fait de communiquer des informations confidentielles sans respecter les procédures particulières de protection et d'autorisation.

○ L'utilisation de l'Internet dans des conditions susceptibles de porter atteinte à l'image ou à la réputation d'autrui ou de l'établissement, et d'une façon générale, d'engager la responsabilité civile ou pénale de l'utilisateur et/ou de l'établissement.

Article 1.3.2 ACCES A LA MESSAGERIE ET A L'INTERNET

L'accès à la messagerie et à l'intranet est réservé à un usage strictement professionnel. En conséquence, tous documents ou tous courriers électroniques transitant par la messagerie, envoyés ou reçus sur l'intranet, notamment dans des forums, sont réputés revêtir un caractère exclusivement professionnel et ne peuvent dès lors être considérés comme une correspondance privée au sens du Code pénal.

Sont notamment considérés comme fautifs ou abusifs les agissements suivants, sans que cette liste ne présente un caractère limitatif :

- | | |
|--|---|
| <ul style="list-style-type: none">○ L'utilisation de la messagerie ou de l'intranet à des fins personnelles.○ Le fait de tenir ou de diffuser, par la messagerie ou par l'intranet, des propos xénophobes, racistes, constitutifs de harcèlement sexuel, injurieux, diffamatoires ou dénigrants et, d'une façon très générale tous propos susceptibles d'engager la responsabilité pénale et/ou civile de son auteur. | <ul style="list-style-type: none">○ La diffusion en chaîne de courriers, les envois automatiques ou en masse ou toute autre distribution à grande échelle.○ Le fait d'envoyer des messages sous le nom d'une autre personne, sauf autorisation de celle-ci.○ Le fait d'envoyer des messages ou documents confidentiels sans respecter les procédures de protection et d'autorisation.○ L'utilisation du réseau à des fins, politiques, religieuses ou sectaires, ou pour exposer publiquement ou en nombre une revendication individuelle ou collective. |
|--|---|

Article 1.3.3 CONSULTATION A TITRE PERSONNEL

A titre exceptionnel et pour satisfaire à des besoins exprès de la vie quotidienne, le salarié peut être amené à utiliser la messagerie professionnelle ou personnelle à des fins personnelles. Un usage raisonnable dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation du courrier électronique n'affecte pas le trafic normal des messages professionnels. Il doit indiquer, à chaque envoi, et faire indiquer par chaque expéditeur le caractère personnel de la correspondance ; à défaut, elle est réputée être professionnelle. Toute utilisation en dehors des cas visés exceptionnels visés caractérise une faute.

Le contenu des sites Internet consultés ne doit pas être contraire à l'ordre public et aux bonnes mœurs. Il ne doit pas mettre en cause l'intérêt et la réputation de l'établissement.

Article 1.3.4 UTILISATION DU MINITEL ET DU TELEPHONE FIXE OU MOBILE

L'utilisation du minitel, du téléphone fixe et du téléphone mobile professionnel est réservée à un usage essentiellement professionnel. En conséquence, chacun s'engage à s'abstenir à faire abusivement utilisation du minitel, du téléphone fixe ou mobile.

Sont notamment considérés comme fautifs ou abusifs les agissements suivants :

- | | |
|---|---|
| <ul style="list-style-type: none">○ L'utilisation du minitel non justifiée par les besoins de la vie quotidienne.○ L'accès à des serveurs à caractère pornographique, xénophobe ou raciste et plus généralement de tout serveur dont l'objet est manifestement étranger à l'exercice par le salarié de son activité au sein de l'entreprise. | <ul style="list-style-type: none">○ L'utilisation du téléphone fixe ou mobile à des fins personnelles, sauf en cas d'urgence. |
|---|---|

1.4. Utilisation de logiciels

L'utilisateur ne peut installer un logiciel. Seul le service informatique est habilité à le faire. Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin et nommée par le responsable de l'établissement.

Par ailleurs l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel, ni développer des programmes constituant ou s'apparentant à des virus.

Article 2 UTILISATION DES INFORMATIONS ET DES SYSTEMES D'INFORMATION

Article 2.1 Condition de confidentialité

L'accès et l'utilisation des informations traitées dans l'établissement doivent s'exercer dans le cadre de l'activité professionnelle de chaque collaborateur, en fonction de son emploi et des objectifs qui lui sont fixés.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégés.

Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec le Directeur de l'établissement ou au Correspondant à la protection des données et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

Sont notamment considérés comme fautifs ou abusifs, les agissements suivants :

- | | |
|--|--|
| <ul style="list-style-type: none">○ Communiquer à un tiers les codes d'accès et les codes secrets des systèmes informatiques, permettre ou faciliter cette communication,.○ Tenter d'obtenir ou obtenir, par quelque moyen que se soit, l'identifiant ou les codes secrets de tiers.○ Accéder ou tenter d'accéder à des serveurs, bases de données, logiciels, quel que soit leur utilisation et leur propriétaire, sans autorisation ou sans rapport avec les missions confiées au salarié. | <ul style="list-style-type: none">○ Utiliser à des fins frauduleuses les informations connues dans le cadre de ses activités professionnelles.○ Copier ou dupliquer à des fins personnelles ou diffuser à des tiers, sous quelque forme que se soit, des données propriétés « Fondation ILDYS ».○ Installer ou utiliser sur le système informatique de la « Fondation ILDYS » des logiciels ou des programmes non justifiés par les intérêts du service, sauf autorisation écrite de la Direction. |
|--|--|

L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

Article 2.2 PRESERVATION DE L'INTEGRITE DES SYSTEMES INFORMATIQUES

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques...

Tout travail de recherche ou autre, risquant de conduire à la violation de la règle définie dans le paragraphe précédent, ne pourra être accompli qu'avec l'autorisation du responsable de l'établissement et dans le strict respect des règles qui auront alors été définies.

ARTICLE 3 CONTROLE ET SANCTION EN CAS D'INOBSERVATION DES DISPOSITIONS DE LA CHARTE

Article 3.1. Contrôle effectué dans le cadre de maintenance et de gestion technique

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et liberté.

Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes sont conduits par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions Internet, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail.

Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978.

Article 3.2. Contrôle en cas d'abus constaté

Afin de garantir l'effectivité des principes définis ci-dessus, l'établissement pourra, en cas d'abus constaté, être amené à exercer des contrôles sur l'utilisation de ces moyens d'information et de communication, dans le respect du droit de vie privée de chacun. Ces contrôles pourront notamment porter sur l'utilisation des différents outils d'information et de communication, le coût et la durée des communications, les relevés des factures, les plages et l'amplitude horaire de connexion, les sites visités, les fichiers téléchargés d'un volume, les adresses des sites web.

Conformément à l'article 24 de la loi informatique et liberté du 6 janvier 1978, les informations collectées font l'objet d'un traitement automatisé.

En cas de constat de pratique illicite ou non conforme du réseau ou de doutes sérieux, l'administrateur devra constituer un dossier suffisamment complet pour attester de cette illégalité ou pour justifier la présomption d'utilisation illicite du réseau. Il avertira ensuite son employeur sans toutefois lui révéler le contenu des messages ou fichiers qui demandera par requête au tribunal compétent l'autorisation de faire procéder à la lecture et /ou à la saisie des fichiers visés.

Si l'employeur pense que l'infraction commise par un de ses salariés au moyen de l'outil mis à disposition par l'entreprise est d'ordre pénale, il se tournera vers la voie pénale. Une plainte au procureur de la république, si elle repose sur des éléments sérieux, entraînera une enquête préliminaire.

Article 3.3. SANCTIONS

Les dispositions de la charte constituent un tout indivisible s'imposant à l'ensemble des salariés de l'établissement.

Le non-respect des principes développés dans la charte informatique constitue une faute passible d'une sanction disciplinaire pouvant aller jusqu'à la rupture du contrat de travail, conformément aux dispositions des articles 30 et 31 du règlement intérieur que le présent avenant vient compléter et convention collective applicables.

ARTICLE 4 ENTREE EN VIGUEUR

La charte informatique entrera en vigueur le 01/03/2006.

Pour la Direction du Site de Perharidy,
Monsieur D. BONNE

Pour la section syndicale C.F.D.T,
Monsieur C. CAVAREC

Pour la section syndicale C.G.T,
Madame M. NUREMBERG

ANNEXE

RAPPEL DES PRINCIPALES LOIS FRANCAISES

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique.

- ⊙ La loi du 06/01/1978 « informatique et liberté » <http://www.cnil.fr>
- ⊙ La législation relative à la fraude informatique <http://www.legifrance.gouv.fr>
- ⊙ La législation relative à la propriété intellectuelle <http://www.legifrance.gouv.fr>
- ⊙ La loi du 04/08/1994 relative à l'emploi de la langue française <http://www.culture.fr>
- ⊙ La législation applicable en matière de cryptologie <http://www.telecom.gouv.fr>